VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Algebraická analýza hlavolamů

Algebraic analysis of puzzles

2019 David Lukáš

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra aplikované matematiky

Zadání bakalářské práce

Student: **David Lukáš**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 1103R031 Výpočetní matematika

Téma: Algebraická analýza hlavolamů
Algebraic analysis of puzzles

Jazyk vypracování: čeština

Zásady pro vypracování:

Většinu klasických hlavolamů lze modelovat vhodnou algebraickou strukturou. Například dobře známou Rubikovu kostku lze popsat pomocí podgrupy permutací nějaké množiny. Potom je možno zkoumat, která rozmíchání jsou přípustná a která nikoliv, kolik různých rozmíchání existuje a nebo kolik nejméně tahů je nutno pro složení kostky.
Podobně lze rozebrat i další známé nebo méně známé hlavolamy. Zpravidla se jedná o náročné netriviální výsledky, cenné proto mohou být i na první pohled jednoduché kroky.

Cílem bakalářské práce je zpracovat přehled známých výsledků pro vybrané hlavolamy a podobné postupy použít i pro rozbor a popis dalších případů. Součástí práce by měly i podrobně komentované příklady.

Práci lze rozdělit do následujících částí:
- studium literatury a elektronických zdrojů
- zpracování přehledu různých známých výsledků
- výběr, prezentace a rozbor dalších vhodných příkladů/hlavolamů

Seznam doporučené odborné literatury:

- J.Gallian: Contemporary Abstract Algebra, Brooks/Cole, (2013). ISBN-10: 1-133-59970-2
- A.Tucker: Applied Combinatorics, Wiley. Sixth Edition, ISBN-13: 978-0-470-45838-9.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **doc. Mgr. Petr Kovář, Ph.D.**

Datum zadání: 01.09.2018

Datum odevzdání: 30.04.2019

prof. RNDr. Jiří Bouchala, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 30. dubna 2019 .....

Souhlasím se zveřejněním této diplomové práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v magisterských programech VŠB-TU Ostrava.

V Ostravě 30. dubna 2019 .....

Rád bych na tomto místě poděkoval všem, kteří mi s prací pomohli, protože bez nich by tato práce nevznikla.

Abstrakt

V této bakalářské práci se budeme zabývat použitím teorie grup k popisu vybraných hlavolamů. Cílem bakalářské práce je souhrn známých poznatků již popsaných hlavolamů a popis struktury dalších hlavolamů. V úvodu sepíšeme základní znalosti z teorie grup. Dále se podíváme na samotné hlavolamy. Nejdříve se podíváme na jednoduché hlavolamy a zkusíme je popsat v zobecněné podobě. Budeme zjišťovat, zda je možné získat všechna možná rozmíchání či rozložení dílků a pokusíme se určit, jak hlavolam vyřešit. Tyto postupy se dále pokusíme použít u složitějších hlavolamů.

Klíčová slova: teorie grup, algebraické struktury, hlavolamy

Abstract

In this bachelor thesis we use group theory for a description of selected puzzles. The purpose of this thesis is to summarize known facts about already described puzzles and to describe other puzzles. In the introduction we list basic definitions and theorems of group theory. In the rest of the work we focus on the puzzles. Firstly, we describe simple puzzles and try to generalize them. We find out if it is possible to find a solution of a puzzle using legal moves while starting from any arrangement of pieces and we also try to determine how to solve the puzzle. Then we try to use these methods for more complex puzzles.

Key Words: group theory, algebraic structurs, puzzles

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V dnešní době existuje nepřeberné množství různých hlavolamů od Loydovy patnáctky, až po velmi známou Rubikovu kostku, která vznikla v roce 1974. Vznik Rubikovy kostky odstartoval éru vývoje hlavolamů. Od jejího proslavení začaly vznikat stovky dalších podobných i méně podobných hlavolamů. Některé z nich jsou například jen větší nebo menší verze Rubikovy kostky, další hlavolamy mohou mít jiné tvary, jako třeba hranol nebo dvanáctistěn. Jiné mohou fungovat na způsob ozubených kol nebo třeba kuliček různých barev, které se mezi sebou dají nějakým způsobem prohazovat.

Většinu z těchto hlavolamů lze modelovat vhodnou algebraickou strukturou. V tomto textu si ukážeme, jak taková struktura vypadá a jak nám pomůže porozumět danému hlavolamu. Popíšeme strukturu několika vybraných hlavolamů a u některých se pokusíme z tohoto popisu vyvodit i postup pro složení hlavolamu. U jednodušších hlavolamů se pokusíme danou strukturu zobecnit, pokud to bude možné.

K tomuto popisu budeme potřebovat znalosti z abstraktní algebry a teorie grup. Proto si na začátku některé poznatky připomeneme a dokážeme věty, které se nám k popisu hlavolamů mohou pomoci.

2 Teorie

V této části práce si shrneme některé poznatky z teorie grup. Budeme pracovat s algebraickými strukturami, popíšeme je a dokážeme vlastnosti, které poté využijeme k popisu hlavolamů. Následující Definice a věty jsme převzali ze studijních materiálů [1]

2.1 Grupa

Definice 2.1 (Kartézský součin) *[1] Kartézským součinem množiny A a B nazveme množinu*

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Definice 2.2 (Binární operace) *[1] Binární operací na množině G nazveme každé zobrazen „$\circ$“*

$$\circ : G \times G \to G.$$

Definice 2.3 (Grupoid) *[1] Nechť G je neprázdná množina a „$\circ$“ binární operace na G. Uspořádanou dvojici $(G, \circ)$ nazveme grupoidem.*

Definice 2.4 (Pologrupa) *[1] Nechť G je neprázdná množina a „$\circ$“ je zobrazení definované na $G \times G$. Pokud platí obě následující vlastnosti*

$$\mathbf{1})\textit{uzavřenost: } \forall a, b \in G : a \circ b \in G,$$
$$\mathbf{2})\textit{asociativita: } \forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c),$$

pak uspořádanou dvojici $(G, \circ)$ nazveme pologrupou.

Definice 2.5 (Neutrální prvek) *[1] Nechť „$\circ$“ je operace na G. Prvek $e \in G$ nazveme neutrálním prvkem vzhledem k operaci „$\circ$“ právě tehdy, když*

$$\forall a \in G : a \circ e = e \circ a = a.$$

Definice 2.6 (Monoid) *[1] Nechť G je neprázdná množina a „$\circ$“ zobrazení definované na $G \times G$. Uspořádanou dvojici $(G, \circ)$ nazveme monoid právě tehdy, když platí*

$$\mathbf{1})\textit{uzavřenost: } \forall a, b \in G : a \circ b \in G,$$
$$\mathbf{2})\textit{asociativita: } \forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c),$$
$$\mathbf{3})\textit{existence neutrálního prvku: } \exists e \in G\ \forall a \in G : a \circ e = e \circ a = a.$$

Definice 2.7 (Inverzní prvek) *[1] Nechť $(G, \circ)$ je grupoid a $e \in G$ je neutrální prvek vzhledem k operaci „$\circ$“. Prvkem inverzním k prvku $a \in G$ vzhledem k operaci „$\circ$“ nazveme prvek $a^{-1} \in G$*

splňující

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Definice 2.8 (Grupa) *[1] Nechť G je neprázdná množina a „$\circ$“ zobrazení definované na $G \times G$. Uspořádanou dvojici $(G, \circ)$ nazveme grupou právě tehdy, když platí*

1) *uzavřenost:* $\forall a, b \in G : a \circ b \in G$,

2) *asociativita:* $\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)$,

3) *existence neutrálního prvku:* $\exists e \in G \, \forall a \in G : a \circ e = e \circ a = a$,

4) *existence inverzí:* $\forall a \in G \, \exists a^{-1} \in G : a \circ a^{-1} = a^{-1} \circ a = e$.

Podívejme se nyní na vlastnosti grup, které vyplývají z definice. Není těžké ukázat, že pokud má prvek inverzi, pak je jediná.

Věta 2.1 (O jednoznačnosti inverzního prvku) *[1] Nechť $(G, \circ)$ je grupa. Potom ke každému prvku existuje právě jeden prvek inverzní.*

Důkaz Postupujeme přímo. Nechť $(G, \circ)$ je grupa a a je libovolný prvek z G. Předpokládejme, že a_1^{-1} i a_2^{-1} jsou prvky inverzní k a. Pak

$$a_1^{-1} = a_1^{-1} \circ e = a_1^{-1} \circ (a \circ a_2^{-1}) = (a_1^{-1} \circ a) \circ a_2^{-1} = e \circ a_2^{-1} = a_2^{-1}.$$

■

Věta 2.2 (O inverzi inverze) *[1] Nechť $(G, \circ)$ je grupa. Potom*

$$\forall a \in G : (a^{-1})^{-1} = a.$$

Důkaz Nechť $(G, \circ)$ je grupa a a je libovolný prvek z G a $a^{-1} \in G$ je inverze k a. Dokažme, že a je inverzní prvek k a^{-1}. Platí

$$a^{-1} \circ a = a \circ a^{-1} = e.$$

Víme tedy, že a je inverze k a^{-1} a podle věty 2.1 a Definice 2.7 tedy víme, že $(a^{-1})^{-1} = a$. ■

0

Věta 2.3 (O krácení v grupě) *[1] Nechť $(G, \circ)$ je grupa. Potom $\forall a, b, c \in G$ platí*

1) $(a \circ c) = (b \circ c) \Rightarrow (a = b)$,

2) $(c \circ a) = (c \circ b) \Rightarrow (a = b)$.

Důkaz Nechť $(G, \circ)$ je grupa a a, b, c jsou libovolné prvky z G. Buď $e \in G$ neutrální prvek vzhledem k „$\circ$“ a $c^{-1} \in G$ inverzní prvek k c. Potom platí

$$\begin{aligned}
&\mathbf{1}) \ (a \circ c) = (b \circ c) \Rightarrow a = a \circ e = a \circ c \circ c^{-1} = b \circ c \circ c^{-1} = b \circ e = b, \\
&\mathbf{2}) \ (c \circ a) = (c \circ b) \Rightarrow a = e \circ a = c^{-1} \circ c \circ a = c^{-1} \circ c \circ b = e \circ b = b.
\end{aligned}$$

■

2.2 Podgrupa

Definice 2.9 (Podgrupa) *[1] Nechť $(G, \circ)$ je grupa. Uspořádanou dvojici $(H, \circ')$ nazveme podgrupou grupy $(G, \circ)$ právě tehdy, když*

$$\begin{aligned}
&\mathbf{1}) \ H \subseteq G, \\
&\mathbf{2}) \ \circ' : H \times H \to G \wedge \forall a, b \in H : a \circ' b = a \circ b, \\
&\mathbf{3}) \ (H, \circ') \textit{ je grupa.}
\end{aligned}$$

Poznámka Nebudeme rozlišovat značení operace na grupě od operace na její podgrupě. Dále tedy budeme značit grupu $(G, \circ)$ a její podgrupu $(H, \circ)$. Je ale důležité vědět, že operace podgrupy $(H, \circ)$ je restrikce operace grupy $(G, \circ)$ na množinu H.

Mějme grupu $(G, \circ)$ a její podgrupu $(H, \circ)$. Podle definice je $(H, \circ)$ sama o sobě grupou. To znamená, že má neutrální prvek. Může se stát, že je neutrální prvek podgrupy $(H, \circ)$ jiný, než neutrální prvek $e_G \in G$? Tedy existuje nějaký prvek $e_H \in H, e_H \neq e_G$? Následující věta nám na tuto otázku odpoví.

Věta 2.4 *[1] Mějme grupu $(G, \circ)$ a její podgrupu $(H, \circ)$ a $e_G \in G$ je neutrálním prvek v $(G, \circ)$. Pak $e_G \in H$ a je neutrálním prvek v $(H, \circ)$.*

Důkaz Mějme grupu $(G, \circ)$ a její podgrupu $(H, \circ)$. $(H, \circ)$ je grupa $\Rightarrow \exists h \in H, e_H \in H : e_H \circ h = h \circ e_H = e_H$. Platí

$$\begin{aligned}
&e_H \circ h = h \\
&e_H \circ h = e_G \circ h \text{ (protože } h \in G \text{ a } e_G \text{ je neutrální prvek v G)} \\
&\quad e_H = e_G \text{ (Díky větě 2.3 o krácení v grupě)}
\end{aligned}$$

■

Ověřovat platnost vlastností z definice je zdlouhavé. Pro zjednodušení můžeme použít následující větu.

Věta 2.5 *[1] Nechť $(G, \circ)$ je grupa a platí*

$$\begin{aligned}
&\textbf{1}) \ H \subseteq G,\\
&\textbf{2}) \ H \neq \emptyset,\\
&\textbf{3}) \ \forall a, b \in H : a \circ b \in H,\\
&\textbf{4}) \ \forall a \in H : a^{-1} \in H.
\end{aligned}$$

Potom $(H, \circ)$ je podgrupou grupy $(G, \circ)$.

Důkaz Ověřme platnosti podmínek z Definice 2.9.

1) $H \subseteq G$.

2) Operace „$\circ$“ na H je restrikce operace „$\circ$“ na množinu G.

3) Podmínky z bodů 2) až 4) představují všechny podmínky kladené na to, aby $(H, \circ)$ byla grupa, s výjimkou asociativity operace a existence neutrálního prvku. Díky větě 2.4 víme, že neutrální prvek v H existuje a je to neutrální prvek grupy$(H, \circ)$. A asociativita operace na H vychází z asociativity operace na G. Protože $(G, \circ)$ je grupa, platí

$$(\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c)) \Rightarrow (\forall a, b, c \in H, \text{ kde } H \subset G \text{ platí } (a \circ b) \circ c = a \circ (b \circ c)).$$

■

Předchozí věta nám dává nástroj, jak poznat, zda je $(H, \circ)$ podgrupou grupy $(G, \circ)$ aniž bychom museli ověřovat, zda $(H, \circ)$ je grupa. Následující věty nám postup ještě zjednoduší.

Věta 2.6 *[1] Nechť $(G, \circ)$ je grupa a platí*

$$\begin{aligned}
&\textbf{1}) \ H \subseteq G,\\
&\textbf{2}) \ H \neq \emptyset,\\
&\textbf{3}) \ \forall a, b \in H : a \circ b^{-1} \in H.
\end{aligned}$$

Potom $(H, \circ)$ je podgrupou grupy $(G, \circ)$.

Důkaz Stejně jako v předchozím důkazu ověříme platnosti podmínek definice 2.9.

1) $H \subseteq G$.

2) Operace „$\circ$“ na H je restrikce operace „$\circ$“ na G.

3) Dokažme, že $(H, \circ)$ je grupa.

a) Z předpokladu je H je neprázdná množina.

b) Vyjdeme z předpokladu **3**) a zvolíme $b = a$. Potom $a \circ a^{-1} = e$. Proto je v H neutrální prvek.

c) $\forall e, a \in H : e \circ a^{-1} = a^{-1}$ (vyšli jsme z předpokladu **3**) a zvolili jsme $a = e$ a $b = a$) Proto v H existují všechny inverze.

d) $\forall a, b \in H : b^{-1} \in H \Rightarrow a \circ (b^{-1})^{-1} = a \circ b \in H \Rightarrow \circ$ je uzavřená na H.

e) Protože $(G, \circ)$ je grupa, platí $(\forall a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c))$. Potom $(\forall a, b, c \in H \subset G (a \circ b) \circ c = a \circ (b \circ c))$.

■

Definice 2.10 *Nechť $(G, \circ)$ je grupa. Buď $a \in G$ a $n \in \mathbb{N}$. Nechť $e \in G$ je neutrální prvek v $(G, \circ)$ a $a^{-1} \in G$ je inverzní prvek k a. Definujme a^n a a^{-n}.*

$$a^n = \begin{cases} e & pro\ n = 0 \\ a & pro\ n = 1 \\ a^{-1} & pro\ n = -1 \\ a^{n-1} \circ a & pro\ n > 1 \\ a^{-n+1} \circ a^{-1} & pro\ n < -1 \end{cases}$$

Poznámka V předchozí definici není důležité, zda operaci „$\circ$“ používáme zleva nebo zprava, jelikož $a^1 \circ a = a \circ a^1 = a^2$, takže $a^{n-1} \circ a = a \circ a^{n-1} = a^n$.

Věta 2.7 *Nechť $(G, \circ)$ je grupa. Buď $a \in G$ a $n \in \mathbb{N}$. Označme neutrální prvek $e \in G$ v $(G, \circ)$ Potom*

$$a^n \circ a^{-n} = a^{-n} \circ a^n = e.$$

Tedy a^{-n} je inverzní prvek k a^n.

Důkaz Tvrzení dokažme přímo. Platí

$$\begin{aligned} a^n \circ a^{-n} &= a^{-n} \circ a^n \\ a^{n-1} \circ a \circ a^{-1} \circ a^{-n+1} &= a^{-n+1} \circ a^{-1} \circ a \circ a^{n-1} \\ a^{n-1} \circ e \circ a^{-n+1} &= a^{-n+1} \circ e \circ a^{n-1} \\ &\vdots \\ a \circ a^{-1} &= a^{-1} \circ a \\ e &= e \end{aligned}$$

■

Věta 2.8 *[1] Nechť $(G, \circ)$ je grupa a platí*

1) $H \subseteq G$,
2) $H \neq \emptyset$,
3) *H je konečná množina*,
4) $\forall a, b \in H : a \circ b \in H$.

Potom $(H, \circ)$ je podgrupou grupy $(G, \circ)$.

Důkaz Díky větě 2.5 stačí dokázat, že $\forall a \in H : a^{-1} \in H$.

$H \neq \emptyset \Rightarrow \exists a \in H$,
1) Pro $a = e$ platí $a^{-1} = a$,
2) Pro $a \neq e$ platí $\forall a, b \in H : a \circ b \in H$, proto $a \in H$, také $a^2 \in H, a^3 \in H, ..., a^i \in H$,
Dále H je konečná, takže$\exists n_1, n_2 \in \mathbb{N}, n_1 > n_2 : a^{n_1} = a^{n_2}, n_1 > n_2 \Rightarrow \exists d \in \mathbb{N} : n_1 = n_2 + d$,
proto

$$\begin{aligned} a^{n_2+d} &= a^{n_2}, \\ a^{n_2} \circ a^d &= a^{n_2}, \\ a^d &= e, \end{aligned}$$

$$a \circ a^{d-1} = a \circ a^{-1} \circ a^d = e, \qquad a^{d-1} \circ a = a^d \circ a^{-1} \circ a = e.$$

Odtud

$$a^{d-1} = a^{-1}.$$

■

2.3 Násobení komplexů a rozklad grupy podle podgrupy

Následující Definice a věty budeme potřebovat pro důkaz Lagrangeovy věty 2.14.

Definice 2.11 (Násobení komplexů) *[1] Komplexem v grupě $(G, \circ)$ nazveme každou podmnožinu množiny G. Nechť $S_1, S_2 \subset G$. Potom definujme*

$$S_1 \circ S_2 = \{s_1 \circ s_2 \mid s_1 \in S_1, s_2 \in S_2\}.$$

V případě, že $S_1 = \{a\}$, $a \in G$ a $S_2 = H, H \subset G$, budeme psát

$$S_1 \circ S_2 = \{a\} \circ H = a \circ H = \{a \circ h \mid h \in H\}.$$

Poznámka V různých textech se můžeme setkat s různým značením operace na grupě. Nejčastější značení je „$\cdot$“ a nazýváme ho násobení, proto násobení komplexů. Někdy se také znaménko operace úplně vynechává, jak jsme zvyklí u klasického násobení. Můžeme tedy vidět například zápis $a \cdot H$ nebo aH. Je třeba si však rozmyslet, že se nejedná o násobení „na číslech“. Operace může být definovaná různě dokonce i na různých prvcích.

Věta 2.9 *[1] Nechť $(G, \circ)$ je grupa a $A, B, H \subseteq G$. Pak*

$$A \circ (B \circ H) = (A \circ B) \circ H.$$

Důkaz Tvrzení dokažme přímo. $(G, \circ)$ je grupa, potom je operace „$\circ$“ asociativní. Pak

$$A \circ (B \circ H) = A \circ \{b \circ h \mid b \in B, h \in H\} = \{a \circ (b \circ h) \mid a \in A, b \in B, h \in H\} =$$
$$= \{(a \circ b) \circ h \mid a \in A, b \in B, h \in H\} = \{a \circ b \mid a \in A, b \in B\} \circ H = (A \circ B) \circ H.$$

■

Násobení komplexů je asociativní.

Definice 2.12 *[1] Nechť $(G, \circ)$ je grupa a $(H, \circ)$ její podgrupa. Pak $G/H = \{a \circ H \mid a \in G\}$ nazýváme rozklad grupy $(G, \circ)$ podle podgrupy $(H, \circ)$ a $|G/H|$ (počet prvků G/H) nazýváme index podgrupy $(H, \circ)$ v podgrupě $(G, \circ)$ a značíme jej $(G : H)$. Přidat příklad.*

Věta 2.10 *[1] Nechť $(G, \circ)$ je grupa a $(H, \circ)$ její podgrupa. Potom*

$$H \circ x = H \Leftrightarrow x \circ H = H \Leftrightarrow x \in H$$

Důkaz Tvrzení budeme dokazovat přímo.
Pro přehlednost vynechme v tomto důkazu značení operace „$\circ$“. Například místo $H \circ x$ budeme psát Hx. Nejdříve dokažme $Hx = H \Leftrightarrow x \in H$.

1) Předpokládejme $Hx = H$. $(H, \circ)$ je grupa, takže má neutrální prvek. Označme ho e. Z definice 2.11 a z předpokladu vyplývá, že $ex \in Hx$. Pak $ex = x$, potom $x \in Hx$ a proto $x \in H$.

2) Předpokládejme $x \in H$.

a) Dokažme, že $Hx \subseteq H$. $(H, \circ)$ je grupa, operace „$\circ$“ je tedy uzavřená na H. Dále vyjdeme z předpokladu. Platí

$$\forall hx \in Hx : hx \in H.$$

Proto $Hx \subseteq H$.

b) Dokažme, že $H \subseteq Hx$. $(H, \circ)$ je grupa a $x \in H$. Určitě tedy existuje $x^{-1} \in H$. Proto platí $\forall h \in H : h = hx^{-1}x$. Označme $hx^{-1} = h_1$. $(H, \circ)$ je grupa, operace „$\circ$“ je tedy uzavřená na H a $x^{-1} \in H$ i $h \in H$. Z toho vyplývá, že $h_1 \in H$. A proto $h_1 x = h, h \in Hx$ a pak $H \subseteq Hx$.

Z bodu **1)** a **2)** vyplývá $Hx = H \Leftrightarrow x \in H$. Nyní dokažme $xH = H \Leftrightarrow x \in H$.

3) Předpokládejme $xH = H$. $(H, \circ)$ je grupa, takže má neutrální prvek. Označme jej e. Z definice 2.11 a z předpokladu vyplývá, že $xe \in xH$. Pak $xe = x$ potom $x \in xH$ a proto $x \in H$.

4) Předpokládejme $x \in H$.

a) Dokažme, že $xH \subseteq H$. $(H, \circ)$ je grupa, operace „$\circ$“ je tedy uzavřená na H. Dále vyjdeme z předpokladu. Platí

$$\forall xh \in xH : xh \in H.$$

Proto $xH \subseteq H$.

b) Dokažme, že $H \subseteq xH$. $(H, \circ)$ je grupa a $x \in H$. Určitě tedy existuje $x^{-1} \in H$. Proto platí $\forall h \in H : h = xx^{-1}h$. Označme $x^{-1}h = h_1$. $(H, \circ)$ je grupa, operace „$\circ$“ je tedy uzavřená na H a $x^{-1} \in H$ i $h \in H$. Z toho vyplývá $h_1 \in H$. A proto $xh_1 = h \in xH$ a pak $H \subseteq xH$.

Z bodů **3)** a **4)** vyplývá, že $xH = H \Leftrightarrow x \in H$. A konečně $Hx = H \Leftrightarrow xH = H$ vyplývá z tranzitivity ekvivalence. ∎

Věta 2.11 *[1] Nechť $(G, \circ)$ je grupa a $(H, \circ)$ její podgrupa. Potom platí*

$$\forall a, b \in G : (a \circ H \cap b \circ H \neq \emptyset) \Rightarrow (a \circ H = b \circ H).$$

Důkaz Tvrzení dokažme přímo.

$$(a \circ H \cap b \circ H \neq \emptyset) \Rightarrow (\exists x \in a \circ H \cap b \circ H) \Rightarrow (\exists h_1, h_2 \in H : x = a \circ h_1 = b \circ h_2) \Rightarrow$$
$$\Rightarrow (a = b \circ h_2 \circ h_1^{-1}) \Rightarrow (\exists h \in H : a = b \circ h) \Rightarrow$$
$$\Rightarrow a \circ H = (b \circ h) \circ H = b \circ (h \circ H) = b \circ H \text{ (z věty 2.10).}$$

■

Důsledek [1] Navzájem různé třídy rozkladu jsou disjunktní.

Věta 2.12 *[1] Nechť $(G, \circ)$ je grupa a $H \subseteq G, H \neq \emptyset$. Potom platí*

$$\bigcup_{a \in G} a \circ H = G.$$

Důkaz Dokážeme přímo.
1) $(G, \circ)$ je grupa, takže operace „$\circ$“ je uzavřená na G. Proto

$$\bigcup_{a \in G} a \circ H \subseteq G.$$

2) Jelikož je H neprázdná množina, jistě existuje prvek $h \in H$. A jelikož je $H \subseteq G$ platí $h \in G$. Tedy

$$H \neq \emptyset \Rightarrow \exists h \in H \Rightarrow \bigcup_{a \in G} a \circ H \supseteq \bigcup_{a \in G} a \circ \{h\} = \{a \circ h \mid a \in G\} = G \circ h = G \text{ (podle věty 2.10).}$$

Z bodů **1)** a **2)** vyplývá

$$G \subseteq \bigcup_{a \in G} a \circ H \subseteq G \Rightarrow G = \bigcup_{a \in G} a \circ H.$$

■

Definice 2.13 (Řád grupy) *[1] Nechť $(G, \circ)$ je grupa. Počet prvků množiny G nazýváme řádem grupy $(G, \circ)$ a značíme jej $|G|$.*

Věta 2.13 *[1] Nechť $(G, \circ)$ je grupa a $(H, \circ)$ je její konečná podgrupa. Potom*

$$\forall (a \circ H) \in G/H : |a \circ H| = |H|.$$

Důkaz Dokážeme přímo. Potřebujeme nalézt bijektivní zobrazení $f : H \to a \circ H$. Dokažme, že $f : f(h) = a \circ h, \forall h \in H$ je bijekce.

1) $\forall h_1, h_2 \in H : f(h_1) = f(h_2) \Leftrightarrow a \circ h_1 = a \circ h_2 \Leftrightarrow h_1 = h_2 \Rightarrow f$ je injektivní zobrazení.

2) $\forall (a \circ h) \in (a \circ H)\ \exists h \in H : f(h) = a \circ h \Rightarrow f$ je surjektivní zobrazení.

Z bodů **1)** a **2)** vyplývá, že f je bijektivní zobrazení. ∎

Definice 2.14 (Řád prvku) *[1] Nechť $(G, \circ)$ je grupa a buď $a \in G$. Nejmenší přirozené číslo n splňující*

$$a^n = e,$$

kde e je neutrální prvek v grupě $(G, \circ)$, nazveme řádem prvku a. Pokud takové číslo neexistuje, říkáme, že a je nekonečného řádu.

Z předchozích tvrzení již snadno odvodíme následující větu.

Věta 2.14 (Lagrangeova) *[1] Nechť $(G, \circ)$ je konečná grupa a $(H, \circ)$ je její podgrupa. Potom platí*

1) $|G| = |G/H| \cdot |H| = (G : H) \cdot |H|$.

2) $|H| \mid |G|$ *(řád podgrupy dělí řád grupy).*

3) *Nechť $n \in \mathbb{N}$ je řád prvku $a \in G$. Potom $n \mid |G|$.*

4) *Nechť $K \subseteq H \subseteq G$, $(K, \circ)$ a $(H, \circ)$ jsou podgrupy grupy $(G, \circ)$. Potom* $|G/K| = |G/H| \cdot |H/K|$.

Důkaz Jednotlivé části budeme dokazovat přímo.

1) $(G, \circ)$ je konečná grupa, proto $(H, \circ)$ je konečná grupa a tak
$\forall a \in G : (|H| = |a \circ H|)$, pak $|G/H| = |\{a \circ H | a \in G\}|$ a proto $|G| = |G/H| \cdot |H|$.

2) Protože $|G| = |G/H| \cdot |H|$, tak $|H| \mid |G|$.

3) Nechť n je řád prvku a. Označme $A = \{a^i \mid i \in \{1, ..., n\}\}$. Pak
$\forall i, j \in \{1, ..., n\} : a^i \circ a^{-j} = a^i \circ a^{-j} \circ e = a^i \circ a^{-j} \circ a^n = a^i \circ a^{n-j} \in A$
A jelikož $a^n = e$, je určitě $A \subseteq G$ a také $A \neq \emptyset$. Podle věty 2.8 je tedy $(A, \circ)$ podgrupou $(G, \circ)$. $|A| = n$ a podle **2)** můžeme psát $n \mid |G|$.

4) $(G, \circ)$ je konečná grupa. Proto

$$|G| = |G/H| \cdot |H|,$$
$$|G| = |G/K| \cdot |K|,$$
$$|H| = |H/K| \cdot |K|.$$

Odtud

$$|G/K| \cdot |K| = |G/H| \cdot |H/K| \cdot |K| \quad / : |K| \ (|K| \neq 0, \text{ protože } (K, \circ) \text{ je grupa})$$
$$|G/K| = |G/H| \cdot |H/K|$$

■

Předchozí věta je velmi důležitá. Důsledek věty například je, že žádný hlavolam o n prvcích nemůže mít libovolný počet možných rozmíchání. Vždy musí být roven $\frac{n!}{d}$, kde $d \in \mathbb{N}$. Například hlavolam o 5 prvcích jistě nemůže mít 110 různých rozmíchání, protože $\nexists d \in \mathbb{N} : 110 = \frac{5!}{d}$.

2.4 Cyklické grupy, generátor

Definice 2.15 (Cyklická grupa, generátor) *[1] Grupu $(G, \circ)$ nazveme cyklickou grupou právě tehdy, když*

$$\exists a \in G : G = \{a^n \mid n \in \mathbb{Z}\}.$$

Prvek a nazýváme generátorem grupy $(G, \circ)$ a značíme $G = \langle a \rangle$.

Definice 2.16 (Grupa generovaná množinou) *[12] Nechť $(G, \circ)$ je grupa a $S \subseteq G$. S nazveme generující množinou grupy $(G, \circ)$ právě tehdy, když*

$$\forall g \in G : g = a_1 \circ a_2 \circ ... \circ a_n,$$

kde $\forall a_i$ platí buď $a_i \in S$ nebo $a_i^{-1} \in S$. Značíme $G = \langle S \rangle$.

2.5 Grupy permutací

Definice 2.17 (Permutace) *[1] Permutací množiny G nazveme každé bijektivní zobrazení*

$$\sigma : G \to G.$$

Věta 2.15 *Nechť $P = \{\sigma : G \to G \mid \sigma \text{ je bijekce}\}$ (to znamená, že P je množina všech permutací množiny G) a $\circ$ je skládání zobrazení. Potom $(P, \circ)$ je grupa a nazveme ji grupa permutací.*

Důkaz Ověříme platnost podmínek z definice 2.8. Následující

1) uzavřenost: Složení dvou bijekcí je bijekce. [2]

2) asociativita: Skládání zobrazení je asociativní. [2]

3) existence neutrálního prvku: Neutrálním prvkem v $(P, \circ)$ je $id \in P$, id je identita. Opravdu, $\forall \pi \in P : id \circ \pi = \pi \circ id = \pi$.

4) existence neutrálních prvků: Protože $\forall \sigma \in P$ platí, že σ je bijekce, proto existuje permutace σ^{-1}, která je inverzí k σ.[2]

■

Poznámka Přestože existují permutace nekonečných množin, nadále se budeme zabývat pouze permutacemi konečných množin.

Definice 2.18 (Symetrická grupa) *[2] Nechť G je konečná množina o n prvcích. Grupu tvořenou množinou všech permutací G a operací „$\circ$“ (skládání permutací), nazveme Symetrickou grupou a značíme ji*

$$(S_n, \circ) = (\{\sigma : G \to G \mid \sigma \textit{ je bijekce}\}, \circ).$$

Původní množinu G značíme I_n.

Úmluva Obecně můžou být prvky množiny $I_n = \{a_1, a_2, ..., a_n\}$ jakékoliv. Pro jednoduchost zápisu však budeme označovat prvek a_1 symbolem 1, prvek a_2 symbolem 2, ... a prvek a_n symbolem n. Budeme tedy značit $I_n = \{1, 2, ..., n\}$. Nadále budeme počítat s tím, že máme množinu I_n a množinu všech jejich permutací S_n.

V některých textech se značí grupa $(S_n, \circ)$ pouze jako S_n. Je jasné, že pro množinu permutací je operací na grupě skládání zobrazení. V jiných textech se vynechává značení operace úplně. Mluví-li se o grupě $(G, \circ)$, značí se pouze jako G.

Pro přehlednější a rychlejší zápis permutací nejčastěji používáme dva způsoby. Tabulkový zápis, kde v horním řádku jsou v pořadí zapsány vstupní hodnoty a ve spodním řádku výsledek permutace. Například máme-li množinu $I_4 = \{1, 2, 3, 4\}$ a permutaci $\sigma : I_4 \to I_4$ definovanou jako $\sigma(1) = 1, \sigma(2) = 4, \sigma(3) = 2, \sigma(4) = 3$, vypadal by její tabulkový zápis takto:

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{smallmatrix}\right).$$

Dalším obvyklým zápisem permutací je zápis pomocí cyklů. Máme-li množinu
$I_6 = \{1, 2, 3, 4, 5, 6\}$ a permutaci $\sigma : I_6 \to I_6$ definovanou jako $\sigma(1) = 1, \sigma(2) = 4, \sigma(3) =$

$2, \sigma(4) = 3, \sigma(5) = 6, \sigma(6) = 5$, můžeme si představit permutaci následovně:

$$\begin{aligned} 1 &\longrightarrow 1, \\ 2 \longrightarrow 4 &\longrightarrow 3 \longrightarrow 2, \\ 5 \longrightarrow\ 6 &\longrightarrow 5. \end{aligned}$$

Teď už stačí, jen vynechat šipky a uzávorkovat.

$$\sigma = (1) \circ (2\ 4\ 3) \circ (5\ 6) = (2\ 4\ 3) \circ (5\ 6).$$

Každá závorka představuje cyklus, obrazem prvku je následující prvek v závorce. Poslední prvek cyklu se zobrazí na první prvek cyklu. Můžete si všimnout, že vynecháváme cykly, které mají pouze jeden prvek.

Definice 2.19 (Transpozice) *[1] Zobrazení $\tau \in S_n, n > 2$ je transpozicí v S_n právě tehdy, když*

$$(\exists j, k \in I_n : \tau(j) = k, \tau(k) = j) \wedge (\forall x \in I_n \setminus \{j, k\} : \tau(x) = x).$$

Transpozice tedy prohodí pouze dva prvky mezi sebou. V cyklickém zápisu můžeme psát $\tau = (j\ k)$. Všimněme si, že v S_n je transpozice vždy sama sobě inverzí. $\tau \circ \tau = id = e$.

Věta 2.16 *[1] Pro každou permutaci $\sigma \in S_n$, kde $n \geq 2$, existují transpozice $\tau_1, \tau_2, ..., \tau_m \in S_n$ takové, že*

$$\sigma = \tau_1 \circ \tau_2 \circ ... \circ \tau_m.$$

Důkaz Budeme dokazovat indukcí podle n.

1) $n = 2$

$I_2 = \{1, 2\} \Rightarrow S_2 = \{id, \tau\},$ kde $\tau = (1\ 2)$ a platí $\tau \circ \tau = id$.

2) Indukční krok. Předpokládejme, že každou permutaci v S_{n-1} lze složit z transpozic z S_{n-1}. Uvažujme libovolné $\sigma \in S_n$.

a) $\sigma(n) = n$. Buď $\sigma^* \in S_{n-1}, \sigma^*(i) = \sigma(i), \forall i \in \{1, ..., n-1\}$. Pak podle předpokladů existují transpozice $\tau_1^*, ..., \tau_m^* \in S_{n-1}$ takové, že $\sigma^* = \tau_1^* \circ ... \circ \tau_m^*$. $\forall i \in \{1, ..., m\}$. Definujme

$$\tau_i(x) = \begin{cases} \tau_i^*(x) & \text{když } x \in I_n \\ n & \text{když } x = n \end{cases},$$

pak $\sigma = \tau_1 \circ ... \circ \tau_2$.

b) $\sigma(n) = k, k \in I_n, 2 < k < n$. Buď $\tau \in S_n : \tau = (k\ n)$. Potom $(\tau \circ \sigma)(n) = \tau(\sigma(n)) = n$. Dále buď $(\tau \circ \sigma)^* \in S_{n-1}, (\tau \circ \sigma)^*(i) = (\tau \circ \sigma)(i), \forall i \in \{1, ..., n-1\}$. Pak podle předpokladů existují transpozice $\tau_1^*, ..., \tau_m^* \in S_{n-1}$ takové, že $(\tau \circ \sigma)^* = \tau_1^* \circ ... \circ \tau_m^*$. $\forall i \in \{1, ..., m\}$. Definujme

$$\tau_i(x) = \begin{cases} \tau_i^*(x) & \text{když } x \in I_n \\ n & \text{když } x = n \end{cases},$$

pak $(\tau \circ \sigma) = \tau_1 \circ ... \circ \tau_2 \Rightarrow \sigma = \tau \circ \tau_1 \circ ... \circ \tau_2$.

■

Příklad Mějme permutaci $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{smallmatrix}\right)$. Najděme nějaké transpozice $\tau_1, ..., \tau_m$, pro které platí, že $\sigma = \tau_1 \circ ... \circ \tau_m$. Nechť $\tau_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{smallmatrix}\right)$ a $\tau_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{smallmatrix}\right)$. Potom

$$\tau_2 \circ \tau_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{smallmatrix}\right) \circ \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{smallmatrix}\right) = \sigma.$$

Definice 2.20 *[1] Buď $\sigma \in S_n$. Označme*

$$\triangle_n = \prod_{a,b \in \{1,...,n\},\ a>b} (a - b)$$

a

$$\sigma\triangle_n = \prod_{a,b \in \{1,...,n\},\ a>b} (\sigma(a) - \sigma(b)).$$

Definice 2.21 *[1] Buď $n \in \mathbb{N}$, $n \geq 2$. Definujme zobrazení $\varepsilon : S_n \to \mathbb{R} \setminus \{0\}$ předpisem*

$$\varepsilon(\sigma) = \frac{\sigma\triangle_n}{\triangle_n}$$

Věta 2.17 *[1] Nechť $\tau \in S_n$ je transpozice. Potom $\varepsilon(\tau) = -1$.*

Důkaz Uvažujme transpozici $\tau \in S_n$, kde $\tau(j) = k, \tau(k) = j$ a $r \in \{1, ..., n\} \setminus \{j, k\}$. Určitě tedy $\tau(r) = r$. Proto platí

1) Jestliže $r > j > k$, pak
$(\tau(r) - \tau(j))(\tau(r) - \tau(k)) = (r - k)(r - j) = (r - j)(r - k)$.

2) Jestliže $j > r > k$, pak
$(\tau(j) - \tau(r))(\tau(r) - \tau(k)) = (k - r)(r - j) = (j - r)(r - k)$.

3) Jestliže $j > k > r$, pak
$(\tau(j) - \tau(r))(\tau(k) - \tau(r)) = (k - r)(j - r) = (j - r)(k - r)$.

4) Navíc platí
$(\tau(j) - \tau(k)) = (k - j) = (-1)(j - k)$.

Z bodů **1**) až **4**) tedy plyne

$$\tau\triangle_n = \prod_{a,b\in\{1,...,n\},\ a>b} (\tau(a) - \tau(b)) = (-1) \cdot \prod_{a,b\in\{1,...,n\},\ a>b} (a - b) =$$

$$= (-1) \cdot \triangle_n \Rightarrow \varepsilon(\tau) = -1.$$

■

Věta 2.18 *[1] Nechť $\sigma \in S_n$ a $\sigma = \alpha_1 \circ \alpha_2 \circ ... \circ \alpha_r = \beta_1 \circ \beta_2 \circ ... \circ \beta_s$, kde $\alpha_1, \alpha_2, ..., \alpha_r$ a $\beta_1, \beta_2, ..., \beta_s$ jsou transpozice z S_n. Potom (r i s je současně sudé) nebo (r i s je současně liché).*

Důkaz Tvrzení dokážeme přímo.

1) $\sigma = \alpha_1 \circ \alpha_2 \circ ... \circ \alpha_r \Rightarrow\ \sigma\triangle_n = (\alpha_1 \circ \alpha_2 \circ ... \circ \alpha_r)\triangle_n = -((\alpha_1 \circ \alpha_2 \circ ... \circ \alpha_{r-1})\triangle_n) =$
$= ((\alpha_1 \circ \alpha_2 \circ ... \circ \alpha_{r-2})\triangle_n) = ... = (-1)^r\triangle_n$.

2) $\sigma = \beta_1 \circ \beta_2 \circ ... \circ \beta_s \Rightarrow \sigma\triangle_n = ((\beta_1 \circ \beta_2 \circ ... \circ \beta_s)\triangle_n) = -((\beta_1 \circ \beta_2 \circ ... \circ \beta_{s-1})\triangle_n) =$
$= ((\beta_1 \circ \beta_2 \circ ... \circ \beta_{s-2})\triangle_n) = ... = (-1)^s\triangle_n$.

Z bodů **1**) a **2**) plyne, že $\varepsilon(\sigma) = (-1)^r = (-1)^s \Rightarrow r$ i s jsou obě sudá čísla nebo obě lichá čísla.

■

Definice 2.22 (Sudé a liché permutace) *[1] Permutaci $\sigma \in S_n$ nazveme*

a) *sudou permutací právě tehdy, když $\varepsilon(\sigma) = 1$.*

b) *lichou permutací právě tehdy, když $\varepsilon(\sigma) = -1$.*

Důsledkem věty 2.18 je, že každá sudá permutace se dá zapsat jako složení sudého počtu transpozic a každá lichá permutace dá napsat jako složení lichého počtu transpozic.

Definice 2.23 *Buď $n \in \mathbb{N}, n \geq 2$. Nechť $A_n \subseteq S_n$ je množina všech sudých permutací z S_n. Grupu $(A_n, \circ)$ nazýváme alternující grupou.*

Ukážeme, že definice je korektní.

Důkaz Dokažme, že $(A_n, \circ)$ je podgrupou $(S_n, \circ)$. Využijeme větu 2.8.

1) $A_n \subseteq S_n$ předpokládáme.

2) Pro $n \geq 2$ jistě platí, že $A_n \neq \emptyset$.

3) A_n je konečná množina, protože $n \in \mathbb{N}$. S_n obsahuje právě $n!$ prvků a A_n určitě nemůže obsahovat více.

4) Nechť σ_1 a σ_2 jsou libovolné permutace z A_n. σ_1 je sudá permutace, dá se tedy vyjádřit jako složení sudého počtu transpozic. σ_2 je také sudá permutace, dá se tedy také vyjádřit jako složení sudého počtu transpozic. Složíme-li σ_1 a σ_2, skládáme sudý počet transpozic se sudým počtem transpozic. Podle věty 2.18 je celkový počet transpozic také určitě sudý. Výsledek je tedy také sudá permutace. Proto můžeme psát $\forall \sigma_1, \sigma_2 \in A_n : \sigma_1 \circ \sigma_2 \in A_n$.

A proto díky větě 2.8 víme, že $(A_n, \circ)$ je podgrupou $(S_n, \circ)$. ∎

Důsledkem Definice 2.23 je, že pokud složíme dvě sudé permutace, jistě dostaneme sudou permutaci.

Následující věty využijeme při určování počtu možných rozložení některých hlavolamů. Tvrzení odvodíme sami.

Věta 2.19 *Mějme $n \in \mathbb{N}$. Označme $K = \{(1, i) \in S_n \mid i \in \{2, ..., n\}\}$. Pak*

$$(\langle K \rangle, \circ) = (S_n, \circ).$$

Důkaz Tvrzení dokážeme přímo. Buď $i, j \in \{2, ..., n\}, i \neq j$. Mějme dvě libovolné permutace $(1\ i), (1\ j) \in K$. Ukažme, že $(i\ j) \in K$.

$$(1\ i) \circ (1\ j) \circ (1\ i) = (i\ j).$$

Skládáním můžeme tedy složit libovolnou permutaci z S_n. Z toho vyplývá, že $(\langle K\rangle, \circ) = (S_n, \circ)$. ■

Poznámka Všimněme si, že pokud 1 nahradíme libovolným pevným prvkem $a \in \{2, ..., n\}$, bude věta analogická stále platit.

Věta 2.20 *Mějme $n \in \mathbb{N}$. Označme $K = \{(1, i, j) \in A_n \mid i, j \in \{2, ..., n\} \ \wedge \ i \neq j\}$. Potom*

$$(\langle K\rangle, \circ) = (A_n, \circ).$$

Důkaz Dokážeme přímo. Buď $i, j, k, l \in \{2, ..., n\}, i \neq j \neq k \neq l$. Mějme dvě libovolné permutace $(1\ k\ i), (1\ i\ j) \in K$. Potom

$$(1\ k\ i) \circ (1\ i\ j) = (i\ j\ k).$$

Tedy můžeme složit jakýkoliv 3-cyklus. Dále

$$(i\ k\ j) \circ (i\ k\ l) = (i\ j) \circ (k\ l).$$

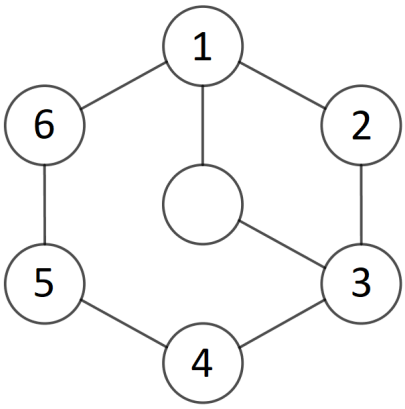
A jelikož každá sudá permutace se dá vyjádřit buď ve formě $(a\ b\ c)$ nebo $(a\ b) \circ (c\ d)$ a také jelikož víme, že kombinací sudých permutací se dá získat jen sudá permutace, víme, že můžeme v grupě vytvořit jakoukoliv sudou permutaci. Z toho vyplývá, že $(\langle K\rangle, \circ) = (A_n, \circ)$.. ■

Poznámka Stejně jako u věty 2.19 si můžeme všimnout, že pokud 1 nahradíme libovolným prvkem $a \in \{2, ..., n\}$, bude věta analogická stále platit.

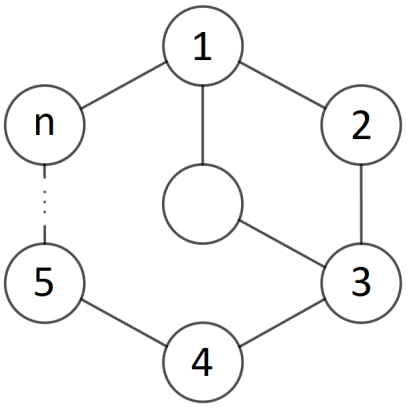
3 Hlavolamy

V této části práce, se podíváme na několik vybraných hlavolamů a popíšeme jejich strukturu algebraicky. Ukážeme si, jak se lze hlavolam modelovat pomocí grupy permutací. Budeme zjišťovat, kolik možných rozmíchání hlavolamu můžeme dosáhnout legálními tahy.

3.1 Hlavolam s pousvnými dísky



Obrázek 1: Hlavolam s posuvnými disky



Obrázek 2: Zobecněný hlavolam s posuvnými disky

První hlavolam, který budeme rozebírat je hlavolam z knížky [2]. Zvolili jsme ho pro jeho jednoduchost. Hlavolam si můžeme prohlédnout na obrázku 1. Hlavolam je složen z šesti disků a volné pozice uprostřed. Každý disk je možno posunout na sousední pozici, pokud je prázdná. Pro zjednodušení si představíme, že každý legální tah musí končit s volným polem uprostřed. Ukážeme si kolika a jakých možných rozmíchání je možné dosáhnout pro obecnou verzi tohoto hlavolamu.

Definice 3.1 (Hlavolam s posuvnými disky) *Definujme hlavolam jako grupu generovanou permutacemi*

$$\sigma_1 = (1\ 3\ 2),$$

$$\sigma_2 = (1\ 3\ 4\ 5\ 6),$$

,kde σ_1 a σ_2 jsou legálními tahy. Prvky odpovídají diskům hlavolamu.

Definice 3.2 (Zobecněný hlavolam s posuvnými disky) *Buď $n \in \mathbb{N}$, $n \geq 4$. Pak je zobecněný hlavolam definovaný jako grupa generovaná permutacemi*

$$\sigma_1 = (1\ 3\ 2),$$

$$\sigma_2 = (1\ 3\ 4\ ...\ n-1\ n),$$

,kde σ_1 a σ_2 jsou legálními tahy. Prvky odpovídají diskům hlavolamu.

Poznámka Permutace σ_2 je tvořena všemi prvky 1 až n, kromě 2.

Hlavolam si můžeme prohlédnou na obrázku 2.

Věta 3.1 *Mějme zobecněný hlavolam s posuvnými disky o n prvcích. Pak pro*

1)*n liché existuje n! různých rozmíchání tohoto hlavolamu legálními tahy.*

2)*n sudé existuje* $\frac{n!}{2}$ *různých rozmíchání tohoto hlavolamu legálními tahy.*

Důkaz Náš zobecněný hlavolam lze modelovat grupou permutací G. Operací je „$\circ$“ (skládání permutací) a množinu G tvoří všechny permutace, které můžeme dostat skládáním σ_1 a σ_2. Potřebujeme tedy dokázat, že pro n liché G obsahuje všechny permutace a pro n sudé G obsahuje polovinu všech permutací.

1) Buď $n \in \mathbb{N}$, $n > 4$, liché. Mějme grupu G reprezentující zobecněný hlavolam o n discích. Ukážeme, jak sestavit všechny permutace $(2\ i)$, kde $i \in \mathbb{N}, i \leq n \wedge i \neq 2$. Začneme tím, že ukážeme, jak můžeme dostat permutaci $\sigma_3 = (2\ 3)$. Podívejme se, čemu se rovná $(\sigma_2 \circ \sigma_1)^{n-2}$

$$\begin{aligned}(\sigma_2 \circ \sigma_1)^{n-2} &= ((1\ 3\ 4\ ...\ n-1\ n) \circ (1\ 3\ 2))^{n-2} = \\ &= ((1\ 4\ 5\ ...\ n-1\ n) \circ (2\ 3))^{n-2}.\end{aligned}$$

Permutace $(1\ 4\ 5\ ...\ n-1\ n)$ je disjunktní s permutací $(2\ 3)$ obsahuje $n-2$ prvků (všechny kromě 2 a 3). Tedy $(1\ 4\ 5\ ...\ n-1\ n)$ zobrazí všechny prvky (kromě 2 a 3) na sebe. A navíc, jelikož je n liché, je i $n-2$ liché. Proto

$$((1\ 4\ 5\ ...\ n-1\ n) \circ (2\ 3))^{n-2} = (2\ 3).$$

Nyní ukažme, čemu se rovná $\sigma_3 \circ \sigma_1$.

$$\sigma_3 \circ \sigma_1 = (2\ 3) \circ (1\ 3\ 2) = (1\ 2).$$

A konečně se podívejme, čemu se rovná $\sigma_2^{(i-3)} \circ \sigma_3 \circ \sigma_2^{-(i-3)}$ pro $i \in \mathbb{N}, i \geq 4$.

i) Permutace $\sigma_2^{-(i-3)}$ zobrazí všechny prvky na prvek o $(i-3)$ pozic v cyklu zpět. Všimněte si, že mimo jiné zobrazí i na 3.

ii) Permutace $\sigma_3 = (2\ 3)$ potom zamění 2 a i.

iii) Permutace $\sigma_2^{(i-3)}$ zobrazí všechny prvky na prvek o $(i-3)$ pozic v cyklu dále. Všimněte si navíc, že $\sigma_2^{(i-3)} \circ \sigma_2^{-(i-3)} = id$.

Složením tedy jistě dostaneme $\sigma_2^{(i-3)} \circ \sigma_3 \circ \sigma_2^{-(i-3)} = (2\ i)$. Dokážeme tedy vyměnit jakýkoliv prvek s prvkem 2. Díky větě 2.19 víme, že v grupě G můžeme dostat libovolnou permutaci. Proto $|G| = n!$.

2) Buď $n \in \mathbb{N}$, $n > 4$, sudé. Mějme grupu G reprezentující zobecněný hlavolam o n discích. Budeme dokazovat přímo. Ukážeme, jak sestavit permutace $(2\ i\ j)$, kde $i, j \in \mathbb{N}, i, j \leq n \wedge i, j \neq 2 \wedge i \neq j$. Podívejme se, čemu se rovná $(\sigma_2 \circ \sigma_1^{-1})^{i-3} \circ \sigma_2^{-(i-3)}$, kde $i \in \mathbb{N}, 4 \leq i \leq n$.

$$\sigma_2 \circ \sigma_1^{-1} = (1\ 3\ 4\ ...\ n-1\ n) \circ (1\ 2\ 3) = (1\ 2\ 4\ ...\ n-1\ n)$$
$$(1\ 2\ 4\ ...\ n-1\ n)^{i-3} \circ (1\ 3\ 4\ ...\ n-1\ n)^{-(i-3)} = (i\ 3\ 2)$$

A nyní se podívejme, čemu se rovná $(i\ 3\ 2)^{-1} \circ (j\ 3\ 2)$, kde $j \in \mathbb{N}, 4 \leq j \leq n \wedge i \neq j$

$$(i\ 3\ 2)^{-1} \circ (j\ 3\ 2) = (2\ j\ i)$$

A díky větě 2.20 víme, že nyní můžeme složit jakoukoliv sudou permutaci. Proto $|G| \geq \frac{n!}{2}$. Dále σ_1 se dá vyjádřit ve formě $(1\ 2) \circ (1\ 3)$, což je složení dvou transpozic. σ_1 je tedy sudá permutace. Podobně σ_2 se dá vyjádřit jako $(1\ n) \circ (1\ n-1) \circ ... \circ (1\ 3)$, což je $n-2$ různých transpozic. Jelikož je n sudé je i $n-2$ sudé, proto je i permutace σ_2. A víme, že složením sudých permutací můžeme získat jen sudou permutaci. Proto $|G| \leq \frac{n!}{2}$. A z toho vyplývá $|G| = \frac{n!}{2}$. ∎

Důkaz věty 3.1 nám také dává návod, jak tento hlavolam složit z jakékoliv dosažitelné pozice.

3.2 Maďarské prstence

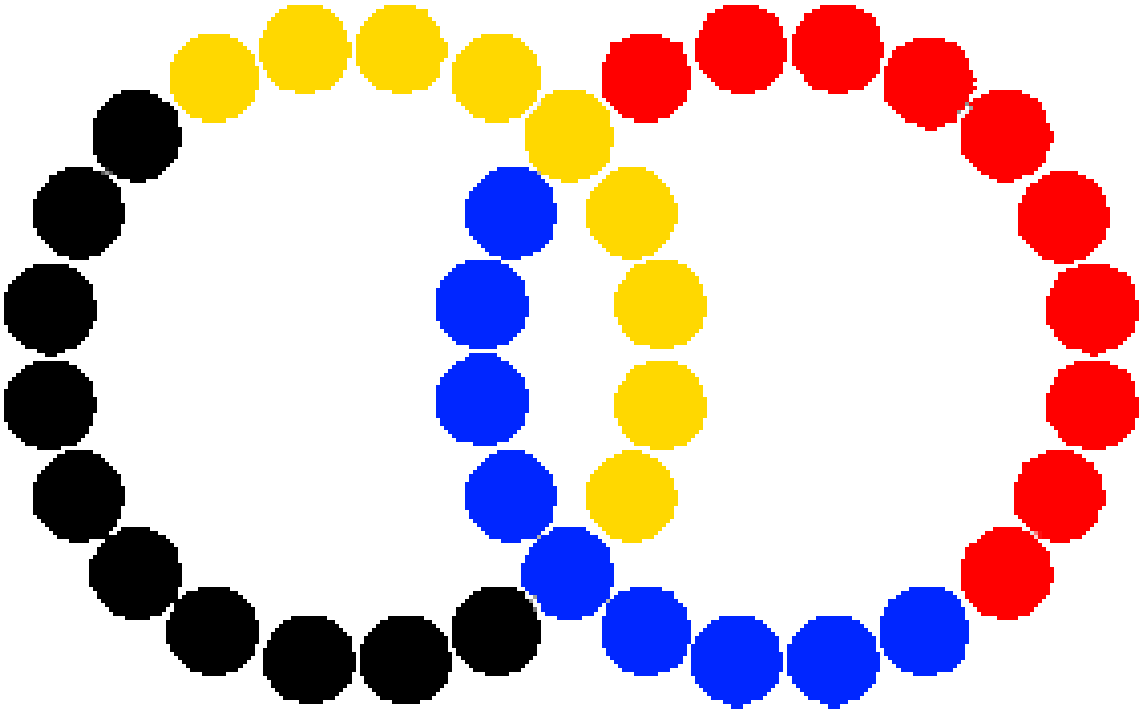
Hlavolam si můžeme prohlédnout na obrázku 3. Všimněme si důležité vlastnosti, kterou hlavolam s posuvnými disky neměl a to je, že korálky nemusí být po složení hlavolamu na stejné pozici, na které začaly, ale mohou si vyměnit pozici s jiným korálkem stejné barvy. Je dobré si tedy klást otázku, zda takovýto hlavolam je možné vyřešit libovolným způsobem, tedy je-li možné přehodit dva korálky a neovlivnit tak zbytek hlavolamu, či nikoliv. Tedy ptáme se zda lze kombinací původních permutací složit transpozici. V případě, že ne, je také dobré zjistit, jaký nejmenší počet korálků můžeme vyměnit. Podíváme se na složitější úlohu – jak by vypadal hlavolam, kdyby měly všechny korálky jinou barvu.

Definice 3.3 (Maďarské prstence) *Definujme hlavolam maďarské prstence jako grupu generovanou permutacemi*

$$a = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20),$$

$$b = (1\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 28\ 29\ 30\ 31\ 32\ 33\ 34\ 6\ 35\ 36\ 37\ 38),$$

kde a a b jsou legálními tahy hlavolamu.



Obrázek 3: Maďarské prstence

Zkusme se nejdříve podívat na zjednodušenou verzi hlavolamu a postupně se propracujme, až k hlavolamu definovanému výše.

Definice 3.4 (Zjednodušené maďarské prstence) *Definujme zjednodušený hlavolam maďarské prstence jako grupu generovanou permutacemi*

$$a = (1\ 2\ 3\ 4\ 5\ 6),$$

$$b = (1\ 2\ 7\ 8\ 9\ 10),$$

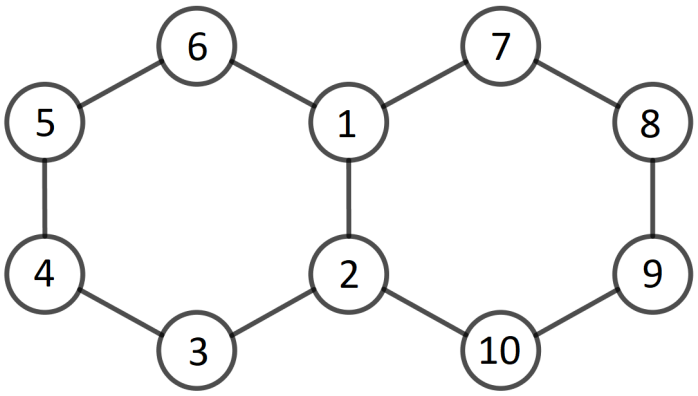
kde a a b jsou legálními tahy hlavolamu.

Hlavolam si můžeme prohlédnout na obrázku 4.

Odvoďme si tvrzení, která nám pomůžou při dokazování věty 3.2. Následující tvrzení odvodíme sami.

Lemma 3.1 (3-cyklus) *Buď $a = (1\ 2\ 3\ 4\ 5\ 6)$, $b = (1\ 2\ 7\ 8\ 9\ 10)$. Pak*

$$(b \circ a^2 \circ b^{-1} \circ a^2)^2 = (2\ 3\ 6).$$



Obrázek 4: Zjednodušené maďarské prstence

Důkaz Tvrzení dokažme přímo. Mějme $a = (1\ 2\ 3\ 4\ 5\ 6)$, $b = (1\ 2\ 7\ 8\ 9\ 10)$. Pak

$$\begin{aligned}(b \circ a^2 \circ b^{-1} \circ a^2)^2 =&(b \circ a^2 \circ (1\ 3\ 5\ 10\ 9\ 8\ 7\ 2\ 4\ 6))^2 = \\ =&(b \circ (1\ 5\ 10\ 9\ 8\ 7\ 4\ 2\ 6\ 3))^2 = \\ =&((1\ 5) \circ (2\ 6\ 3) \circ (4\ 7))^2 = \\ =&(2\ 3\ 6).\end{aligned}$$

■

Lemma 3.2 (2-cyklus) *Buď* $a = (1\ 2\ 3\ 4\ 5\ 6)$, $b = (1\ 2\ 7\ 8\ 9\ 10)$. *Označme* $\sigma = (2\ 3\ 6)$. *Pak*

$$(a^{-1} \circ \sigma)^3 = (1\ 6).$$

Důkaz Tvrzení dokažme přímo. Mějme $a = (1\ 2\ 3\ 4\ 5\ 6)$, $b = (1\ 2\ 7\ 8\ 9\ 10)$. Pak

$$((1\ 2\ 3\ 4\ 5\ 6)^{-1} \circ (2\ 3\ 6))^3 = ((1\ 6) \circ (3\ 5\ 4))^3 = (1\ 6).$$

■

Nyní můžeme dokázat následující tvrzení.

Věta 3.2 *Mějme zjednodušené maďarské prstence. Označme grupu generovanou permutacemi* a, b *jako* $G = (< a, b >, \circ)$. *Pak*

$$G = S_{10}.$$

Důkaz Tvrzení dokažme přímo. Mějme zjednodušené maďarské prstence. Označme $\sigma = (1\ 6)$. Pak

$$b^{-(11-i)} \circ \sigma \circ b^{11-i} = (i\ 6), i \in \{7, 8, 9, 10\},$$

$$\sigma \circ (a^{-1} \circ b)^{6-i} \circ \sigma \circ (b^{-1} \circ a)^{6-i} \circ \sigma = (i\ 6), i \in \{2, 3, 4, 5\}.$$

A díky větě 2.19 o symetrických grupách tedy víme, že $G = S_{10}$. ∎

Nyní se podívejme na strukturu původního hlavolamu z obrázku 3. Následující tvrzení nám poslouží k důkazu věty 3.3. Důkaz těchto tvrzení je inspirován [11]

Lemma 3.3 *[11] Nechť* $a = (1\ ...\ 20)$, $b = (1\ 21\ 22\ 23\ ...\ 34\ 6\ 35\ 36\ 37\ 38)$. *Označme* $c = (b \circ a^{-1} \circ b \circ a)^3$. *Pak*

$$b^4 \circ c \circ b^5 \circ c = (1\ 5\ 30\ 20).$$

Důkaz Tvrzení dokažme přímo. Nechť $a = (1\ ...\ 20)$, $b = (1\ 21\ 22\ 23\ ...\ 34\ 6\ 35\ 36\ 37\ 38)$. Označme $c = (b \circ a^{-1} \circ b \circ a)^3$. Pak

$$c = (b \circ a^{-1} \circ b \circ a)^3 =$$
$$= (1\ 25\ 31\ 35\ 21\ 27\ 33\ 37\ 23\ 29\ 6) \circ (5\ 20\ 26\ 32\ 36\ 22\ 28\ 34\ 38\ 24\ 30),$$

$$b^4 \circ c \circ b^5 \circ c =$$
$$= b^4 \circ c \circ (1\ 30\ 5\ 20\ 31\ 21\ 32\ 22\ 33\ 23\ 34\ 24\ 6\ 25\ 35\ 26\ 36\ 27\ 37\ 28\ 38\ 29) =$$
$$= b^4 \circ (1\ 5\ 26\ 22\ 37\ 34\ 30\ 20\ 35\ 32\ 28\ 24) \circ (6\ 31\ 27\ 23\ 38) \circ (21\ 36\ 33\ 29\ 25) =$$
$$= (1\ 5\ 30\ 20).$$

∎

Lemma 3.4 *[11] Tvrzení dokažme přímo. Nechť* $a = (1\ ...\ 20)$,
$b = (1\ 21\ 22\ 23\ ...\ 34\ 6\ 35\ 36\ 37\ 38)$. *Označme* $\sigma = (1\ 5\ 30\ 20)$. *Pak*

$$(b \circ a^{-6} \circ b^{-1} \circ a)^{-1} \circ b^{-5} \circ a^{-5} \circ b^5 \circ a^5 \circ (b \circ a^{-6} \circ b^{-1} \circ a) \circ \sigma = (1\ 30).$$

Důkaz Tvrzení dokažme přímo. Nechť $a = (1\ ...\ 20)$, $b = (1\ 21\ 22\ 23\ ...\ 34\ 6\ 35\ 36\ 37\ 38)$. Označme $\sigma = (1\ 5\ 30\ 20)$. Pak

$$(b \circ a^{-6} \circ b^{-1} \circ a) =$$
$$= (1\ 16\ 11\ 35\ 20)(2\ 17\ 12\ 7)(3\ 18\ 13\ 8)(4\ 19\ 14\ 9)(5\ 6\ 21\ 15\ 10),$$

$$b^{-5} \circ a^{-5} \circ b^5 \circ a^5 = (1\ 16) \circ (6\ 30),$$

$$(b \circ a^{-6} \circ b^{-1} \circ a) \circ \sigma =$$
$$= (1\ 6\ 21\ 15\ 10\ 5\ 30) \circ (2\ 17\ 12\ 7) \circ (3\ 18\ 13\ 8) \circ (4\ 19\ 14\ 9) \circ (11\ 35\ 20\ 16),$$

$$(1\ 16) \circ (6\ 30) \circ (b \circ a^{-6} \circ b^{-1} \circ a) \circ \sigma =$$
$$= (1\ 30\ 16\ 11\ 35\ 20) \circ (2\ 17\ 12\ 7) \circ (3\ 18\ 13\ 8) \circ (4\ 19\ 14\ 9) \circ (5\ 6\ 21\ 15\ 10),$$

$$(b \circ a^{-6} \circ b^{-1} \circ a)^{-1} \circ (1\ 16) \circ (6\ 30) \circ (b \circ a^{-6} \circ b^{-1} \circ a) \circ \sigma = (1\ 30).$$

■

A nyní můžeme pomocí předchozích tvrzení dokázat následující větu.

Věta 3.3 *Mějme hlavolam maďarské prstence. Označme grupu generovanou permutacemi a, b jako $G = (< a, b >, \circ)$. Pak*

$$G = S_{38}.$$

Důkaz Mějme hlavolam maďarské prstence. Označme $\sigma = (1\ 30)$. Ukažme, jak vypadají permutace $(i, 30)$, pro různá i. Pak

$$a^{-(21-i)} \circ \sigma \circ a^{(21-i)} = (i\ 30), i \in \{1, ..., 20\},$$

a také

$$(b^i \circ a^{-i} \circ b^{-i} \circ a^i) \circ \sigma \circ (a^{-i} \circ b^i \circ a^i \circ b^{-i}) = (i\ 30), \text{ pro } i \in \{21, ..., 34\} \setminus \{25, 30\},$$

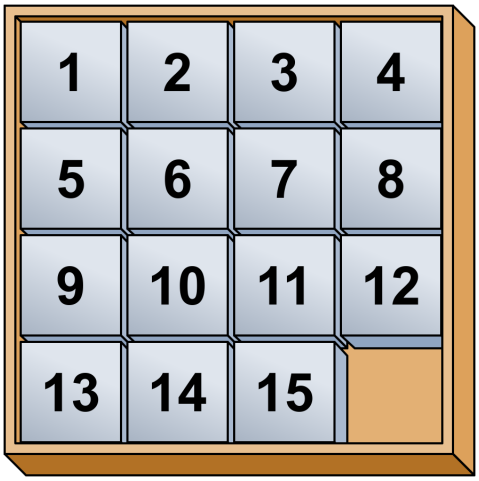
dále

$$(b^i \circ a^{-i} \circ b^{-i} \circ a^i) \circ \sigma \circ (a^{-i} \circ b^i \circ a^i \circ b^{-i}) = ((i-1)\ 30), \text{ pro } i \in \{36, 37, 38, 39\},$$

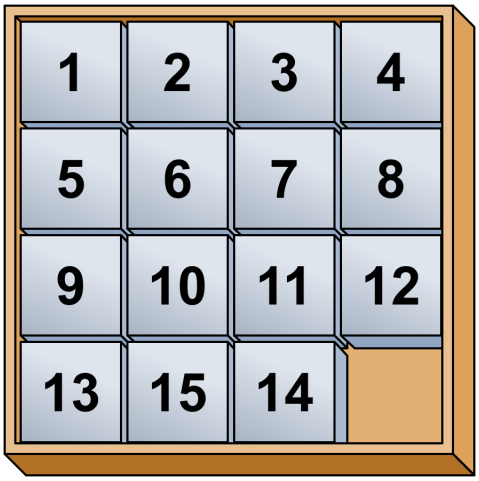
a konečně pro $i = 25$

$$(b^5 \circ a^{-5} \circ b^{-5}) \circ \sigma \circ (b^5 \circ a^5 \circ b^{-5}) = (25, 30).$$

A díky větě 2.19 o symetrických grupách tedy víme, že $G = S_{38}$. ■



Obrázek 5: Patnáctka



Obrázek 6: Rozložená patnáctka

3.3 Loydova patnáctka

Loydova patnáctka nebo také jen patnáctka je velmi populární hlavolam. Do nedávna byl za autora a popularizátora označován Sam Loyd, po němž je hlavolam pojmenován. Ovšem ten neměl s jeho vytvořením ani popularitou nic společného. Na vrcholu slávy byla patnáctka v roce 1880, zatímco Loyd o hlavolamu napsal poprvé až o více než desetiletí později. V roce 1891 se nazval autorem patnáctky ve své knížce Cyclopedia of Puzzles. Skutečným vynálezcem byl však Noyes Chapman, který podal žádost o patent v březnu roku 1880. [4][5]

Hlavolam v složeném stavu je zobrazen na obrázku 5. Je tvořen 15 dílky, které jsou poskládány v krabičce s volnou pozicí na 16 dílek. Cílem je dostat rozmíchaný hlavolam do složeného stavu pouze posouváním dílků na sousední volnou pozici. Nesmí se tedy například žádný dílek vytáhnout. Loyd nabídl cenu 1000 dolarů komukoliv, komu se podaří hlavolam složit z pozice, kde jsou prohozené dílky 14 a 15 (obrázek 6). Nyní si ukážeme, že toto není možné. V zbytku této kapitoly budeme čerpat z [6].

Zaveďme si nejdříve značení pro náš hlavolam. Označíme-li volné pole v patnáctce číslem 16, můžeme každé rozmíchání popsat permutací z S_{16}. Hlavolam ve složeném stavu odpovídá permutaci $\sigma_1 = id$, a hlavolam, který je znázorněn tabulkou 2 odpovídá permutaci $\sigma_2 = (14\ 15)$. Rozmíchání znázorněné tabulkou 3, odpovídá permutaci

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 2 & 15 & 4 & 11 & 5 & 3 & 1 & 8 & 6 & 13 & 12 & 16 & 10 & 14 & 9 & 7 \end{pmatrix}.$$

Budeme-li chtít v tomto rozmíchání posunout například dílek 8 na volnou pozici jedná se složení transpozice $\tau = (7\ 8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 8 & 7 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \end{pmatrix}$ s permutací σ, neboli

$$\tau \circ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 8 & 7 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 2 & 15 & 4 & 11 & 5 & 3 & 1 & 8 & 6 & 13 & 12 & 16 & 10 & 14 & 9 & 7 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 2 & 15 & 4 & 11 & 5 & 3 & 1 & 7 & 6 & 13 & 12 & 16 & 10 & 14 & 9 & 8 \end{pmatrix}.$$

Všimněme si, že jakýkoliv legální tah je transpozice, která prohazuje zvolený prvek, s prvkem, na který je zrovna zobrazený prvek 16.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Tabulka 1: Patnáctka v složeném stavu

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Tabulka 2: Patnáctka s prohozenými dvěma dílky

7	1	6	3
5	9		8
15	13	4	11
10	14	2	12

Tabulka 3: Náhodné rozmíchání patnáctky

Věta 3.4 *Není možné dostat se z rozmíchání z tabulky 2 do složeného stavu z tabulky 1 legálními tahy.*

Důkaz Důkaz provedeme sporem. Předpokládejme, že je možné složit hlavolam z rozmíchání z tabulky 2. Již víme, že každý legální tah má tvar $\tau_{i,16} = (i\ 16)$, kde $i \in \{1, ..., 15\}$. Rozmíchání znázorněné tabulkou 2 odpovídá permutaci $\tau = (14\ 15)$. Musí tedy existovat $\tau_1, \tau_2, ..., \tau_r \in S_{16}, r \in \mathbb{N}$ takové, že $(14\ 15) = \tau_1 \circ \tau_2 \circ ... \circ \tau_r$, kde r udává počet tahů.

Jelikož je volné pole na stejné pozici v obou rozmíchaní znázorněné tabulkami 5 a 6, muselo se po všech tazích $\tau_1 \circ \tau_2 \circ ... \circ \tau_r$ volné pole posunout nahoru tolikrát, kolikrát se muselo posunout dolů a stejně tak se muselo posunout vlevo tolikrát, kolikrát se muselo posunout vpravo. Číslo r tedy musí být jistě sudé. A díky větě 2.18 tedy víme, že $\tau_1 \circ \tau_2 \circ ... \circ \tau_r$ je sudá permutace. Také víme, díky větě 2.17, že $\tau = (14\ 15)$ je lichá permutace. A to je spor. ∎

Podívejme se nyní na strukturu tohoto hlavolamu. Již jsme dokázali, že nemůžeme prohodit libovolné dva dílky - použitím stejného postupu, jako v důkazu věty 3.4 pro všechny ostatní dvojice dílků. Můžeme se ptát, jestli je tedy možné dosáhnout všech sudých permutací. Pro následující část kapitoly lehce pozměníme značení našeho hlavolamu. Pro zjednodušení si představíme, že po dokončení sekvence tahů vždy vrátíme prázdné pole do pravého dolního rohu, podobně jako hlavolamu z kapitoly 3.1. Rozmíchání hlavolamu pak odpovídá permutacím z S_{15}.

Následující tvrzení použijeme pro důkaz věty 3.5. Budeme čerpat z [13]

Lemma 3.5 *V patnáctce je možné dosáhnout rozmíchání $\sigma = (11\ 12\ 15)$ legálními tahy.*

Důkaz Tvrzení dokážeme přímo. Zaměřme se pouze na tato čtyři políčka hlavolamu. V složeném stavu vypadají následovně

11	12
15	

.

Hledanou permutaci získáme těmito kroky

11	
15	12

$\rightarrow$

	11
15	12

$\rightarrow$

15	11
	12

$\rightarrow$

15	11
12	

■

Lemma 3.6 *V patnáctce je možné dosáhnout rozmíchání* $\sigma = (1\ 2\ 3\ 4\ 8\ 15\ 7\ 6\ 10\ 14\ 13\ 9\ 5)$ *legálními tahy.*

Důkaz Tvrzení dokážeme přímo Začněme aplikování permutace (11 12 15) a posunutím pole 11 dolů. Získáme

15	
12	11

.

Nyní postupně posouváme jednotlivé disky tímto způsobem. 8 a 4 posuneme dolů, $3, 2$ a 1 doprava, $5, 9$ a 13 nahoru, 14 doleva, 10 a 6 dolů, 7 doleva 15 nahoru a 8 doleva. Získáváme toto rozložení

5	1	2	3
9	7	15	4
13	6	8	
14	10	12	11

.

Nyní už jen stačí posunout disky 11 a 12 na své místo. Posuneme pole 11 nahoru a aplikujeme permutaci $(11\ 12\ 15)^{-1} = (11\ 12\ 15)^2$. Dostáváme

5	1	2	3
9	7	15	4
13	6	11	12
14	10	8	

,

což je hledaná permutace. ■

Věta 3.5 *Označme* P *množinu všech permutací, které můžeme získat legálními tahy v patnáctce. Potom platí*

$$P = A_{15}.$$

Důkaz Dokážeme přímo. Ukažme, že můžeme najít permutaci $(12\ i\ j)$. Označme $\sigma = (1\ 2\ 3\ 4\ 8\ 15\ 7\ 6\ 10\ 14\ 13\ 9\ 5))$ a $\tau = (11\ 12\ 15)$. Buď $i \in \{1, ..., 15\} \setminus \{11, 12\}$. Pro každé takové i, jistě existuje r takové, že permutace σ^r dostane pole i na pozici 15. Začněme tedy tím, že aplikujeme σ^r. Připomeňme, že σ nemění pole 11 a 12. Dále aplikujme τ. Pole i je nyní na pozici 11. Aplikujeme-li nyní σ^{-r}, vrátíme všechny prvky, kromě $i, 11$ a 12, na původní místo. Konkrétně prvek i je na pozici 11, 11 je na pozici 12 a 12 je na pozici i. Získáváme tedy permutaci $(11\ 12\ i)$. Dále mějme libovolné $j, k \in \{1, ..., 15\} \setminus \{11, 12\}, i \neq j \neq k \neq i$. Pak

$$\begin{aligned}(11\ 12\ k) \circ (11\ 12\ j) &= (11\ k) \circ (12\ j),\\ (11\ 12\ k) \circ (11\ 12\ i) &= (11\ k) \circ (12\ i),\\ (11\ k) \circ (12\ j) \circ (11\ k) \circ (12\ i) &= (12\ i\ j).\end{aligned}$$

Můžeme tedy dostat libovolnou permutaci $(12\ i\ j)$, kde $i, j \in \{1, ..., 15\} \setminus \{12\}, i \neq j$. A díky větám 2.20 a 3.4 již můžeme psát, že $P = A_{15}$. ∎

Dokázali jsme, že v tomto hlavolamu můžeme dosáhnout všechna možná rozmíchání, která odpovídají sudým permutací dílků. Důkaz předchozí věty nám také dává návod, jak patnáctku složit. Tento postup je však velmi zdlouhavý. Nejdříve musíme dostat prvky 11 a 12 na svou pozici. Můžeme se o to pokusit vlastní silou, nebo můžeme použít postup z důkazu věty 3.5. Nejdříve aplikujeme σ^{r_1} tak, abychom dostali prvek 12 na pozici 15, poté aplikujeme τ. Nyní můžeme aplikovat $sigma^{-r_1}$, ale jistě to není potřeba. Dále aplikujeme σ^{r_2} tak, abychom dostali prvek 12 na pozici 15, poté aplikujeme τ. Nyní jsou prvky 11 a 12 na svém místě. Nyní si vybereme náhodný prvek i, který není na svém místě. Řekněme, že je na pozici j. Aplikujme permutaci $(12\ j\ i)$, což je kombinace permutací σ a τ. Nyní je prvek, který byl na pozici i na pozici 12. Označme ho, k. Stačí aplikovat permutaci $(12, k, j)$. Nyní jsou prvky i, k a 12 na své pozici. Nyní vybereme další náhodný prvek, který není na svém místě a postup opakujeme. Tento postup je však velmi neefektivní. Lepší metodu můžeme najít například na [3].

4 Další hlavolamy

V této části bakalářské práce zmíníme další příklady hlavolamů. Ukážeme, jakým způsobem se hlavolam používá, kolik je možných rozmíchání hlavolamu a kolik minimálně tahů potřebujeme pro jejich složení. Nebudeme již však daná tvrzení dokazovat. V této kapitole budeme pracovat s pojmem minimax. Mějme množinu M obsahující minimální počty tahů pro každé rozmíchání hlavolamu. Potom je hodnota minimax rovna maximu množiny M. Někdy se hodnota minimax, označuje také jako „God's number".

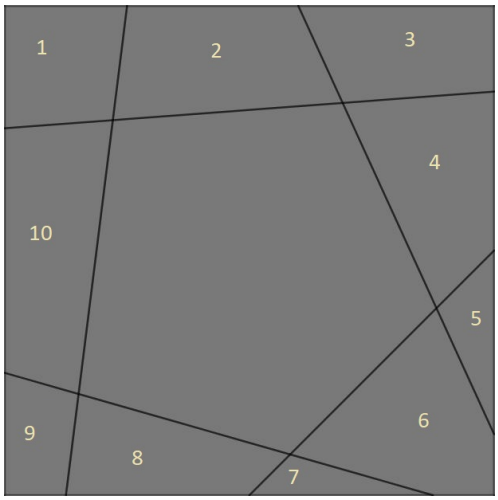
4.1 Hlavolam Floppy Ghost Cube

Obrázek 7: Hlavolam Floppy Ghost Cube

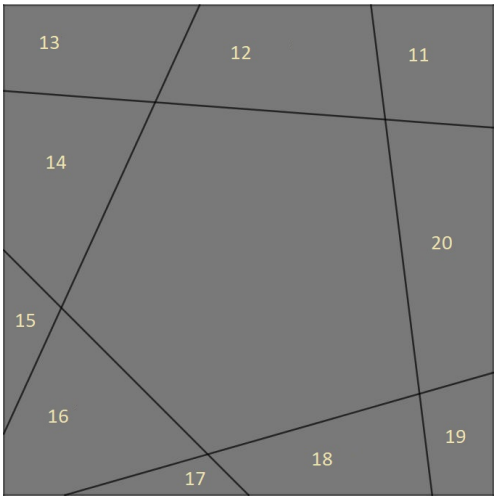
Po vynálezu Rubikovy kostky vznikly stovky podobných i méně příbuzných hlavolamů. Jedním z nich je i hlavolam, který je pojmenován Floppy Ghost Cube. Můžeme si jej prohlédnout na obrázku 7. Jedná se o jeden z hlavolamů, které při skládání mění svůj tvar. Je tvořen nehybným středem, pěti hranovými díly a pěti rohovými díly. Cílem je dostat hlavolam z rozložené podoby do tvaru, jako je na obrázku 7. Jednotlivé tahy jsou tvořeny otočením strany, tvořící hranu a dva sousední rohy, o 180°. Označme stěny hlavolamu tak, jako je to na obrázcích 8 a 9. Nyní

můžeme nadefinovat jednotlivé permutace hlavolamu takto

$$\sigma_1 = (1\ 13) \circ (2\ 12) \circ (3\ 11),$$
$$\sigma_2 = (3\ 15) \circ (4\ 14) \circ (5\ 13),$$
$$\sigma_3 = (5\ 17) \circ (6\ 16) \circ (7\ 15),$$
$$\sigma_4 = (7\ 19) \circ (8\ 18) \circ (9\ 17),$$
$$\sigma_5 = (9\ 11) \circ (10\ 20) \circ (1\ 19).$$



Obrázek 8: Přední stěna hlavolamu Floppy Ghost Cube



Obrázek 9: Zadní stěna hlavolamu Floppy Ghost Cube

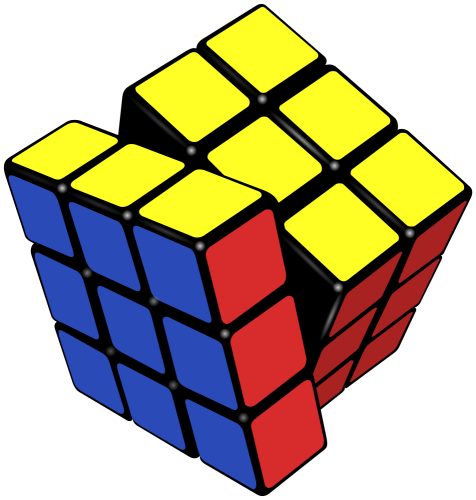
Počet všech možných rozmíchání hlavolamu je 30720. Každá permutace mění právě jednu hranu a 2 rohy. Hrana však zůstává na místě. Legálními tahy můžeme dosáhnout všech 5! permutací rohů. Dále je možné na místě otočit dva rohy nebo dvě hrany. Jeden roh však nelze. Pokud bychom mohli otočit jeden roh na místě, šlo by o 2^5 permutací, musíme však polovinu všech permutací odebrat, proto $2^{5-1} = 2^4$. To samé platí i pro hrany. Celkový počet možných rozmíchání je tedy $5! \cdot 2^4 \cdot 2^4 = 30720$. [7]

Hodnota minimax je 15. V tabulce 4 můžeme kolik tahů je potřeba pro všechna možná rozložení. [7]

Počet tahů	počet rozmíchání
0	1
1	5
2	15
3	40
4	105
5	275
6	670
7	1500
8	3140
9	5825
10	7752
11	6415
12	3395
13	1270
14	282
15	30

Tabulka 4: Minimální počet tahů pro složení každého rozložení hlavolamu Floppy Ghost Cube

4.2 Rubikova kostka



Obrázek 10: Rubikova kostka

Obrázek 11: Rozložená Rubikova kostka

Rubikova kostka je jeden z nejznámějších hlavolamů této doby. Je pojmenován po svém tvůrci Erno Rubikovi, který ji vynalezl v roce 1974. Sám Erno Rubik nejdříve hlavolam nedokázal vyře-

šit a trvalo mu měsíc, než kostku poprvé složil. Hlavolam si můžeme prohlédnout na obrázku 10. Hlavolam je složený z šesti středů, osmi rohů a dvanácti hran. Každá stěna hlavolamu se dá otočit a změní se tak poloha jednotlivých malých kostiček. Rozložený hlavolam můžete vidět na obrázku 11. [8]

Spočítejme, kolik různých rozmíchání je možné dostat. Je možné dosáhnout všech 8! permutací rohů. Navíc má každý roh tři barvy, tedy tři různá možná otočení neboli orientací. To znamená existuje 3^8 různých orientací rohů, ale jen 3^7 orientací je možné dosáhnout, jelikož poslední roh závisí na tom, jak jsou otočeny ostatní. Dále z 12! možných permutací hran. Navíc má každá hrana dvě barvy, takže dvě různá možná otočení. Tedy existuje 2^{12} různých orientací hran, ale orientace poslední hrany závisí na orientaci ostatních hran. To znamená, že je možné dosáhnout 2^{11} orientací hran. Ještě nám ale chybí odebrat polovinu rozmíchání, jelikož parita, neboli sudost či lichost, rohů a hran na sobě závisí. Konkrétně musí být parita permutací rohů stejná jako parita permutací hran. Celkový počet permutací je tedy $\frac{8!\cdot 3^7 \cdot 12!\cdot 2^1 1}{2} = 43\,252\,003\,274\,489\,856\,000 \doteq 4,3 \cdot 10^{19}$. [9]

Podívejme se nyní, jaká je hodnota minimax. Nejdříve si musíme ujasnit, co je jeden tah na Rubikově kostce. Existují dvě metriky. V první je jeden tah každé otočení libovolné stěny o 90°. V druhé metrice, která je častěji používaná, je jeden tah otočení libovolné stěny o 90° nebo 180°. V první metrice je hodnota minimax 26 a v druhé metrice je hodnota minimax 20. Jedním zajímavým rozložením Rubikovy kostky je takové rozložení, u kterého jsou všechny rohy na svém místě a správně orientované a hrany jsou všechny na svém místě, ale všechny jsou špatně orientované. Na toto rozložení je potřeba 20 tahů v druhé metrice, ale pouze 24 tahů v první metrice. [10]

5 Závěr

V této bakalářské práci jsme se zabývali použitím teorie grup k popisu několika vybraných hlavolamů. V úvodu jsme si shrnuli poznatky z teorie grup. Definovali jsme pojem grupa a podgrupa a ukázali jejich některé vlastnosti. Dále jsme si zavedli pojmy a ukázali tvrzení, které nám pomohli dokázat Lagrangaeovu větu, díky které víme, že řád podgrupy dělí řád grupy. Pokračovali jsme zavedením grupy permutací a odvozením vlastností permutací, které nám pomůžou popsat strukturu hlavolamů.

V další části práce jsme si popsali strukturu tří hlavolamů. Začali jsme hlavolamem s posuvnými disky, u kterého se nám podařilo popsat strukturu jeho zobecněné verze. Zjistili jsme, že u tohoto hlavolamu záleží na tom, zda je počet prvků lichá nebo sudý. Přesněji, zda jsou permutace, které znázorňovaly legální tahy hlavolamu, sudé nebo liché permutace. Pokračovali jsme hlavolamem maďarské prstence. Zde jsme nejdříve popsali strukturu jeho zjednodušené verze a dokázali jsme, že u tohoto hlavolamu můžeme dosáhnout všech rozmíchání za pomocí pouze legálních tahů jak u zjednodušené verze hlavolamu, tak i u samotného hlavolamu. Hlavolam se nám však nepodařilo zobecnit. Nakonec jsme se podívali na strukturu známe Loydovy patnáctky. Ukázali jsme, slavnou verzi hry s prohozeným čtrnáctým a patnáctým dílkem nelze vyřešit za pouze pomocí legálních tahů. Také jsme dokázali, že v hlavolamu je možné dosáhnout poloviny všech rozmíchání. Výsledky Loydovy patnáctky a částečně i hlavolamu maďarské prstence jsme převzali z [4], [5], [6], [11] a [13].

V poslední části práce, jsme popsali dva další hlavolamy. Čerpali jsme z [7], [8], [9], [10] U hlavolamu známému jako Floppy Ghost Cube, jsme vypočítali, že celkový počet rozmíchání hlavolamu je 30720, a také jsme si řekli, že se dá z jakékoliv pozice složit do patnácti tahů. A nakonec jsme popsali Rubikovu kostku. Podívali jsme se, kolik možných rozmíchání hlavolamu je možné dosáhnout. Také jsme zjistili, že hlavolam se dá z každého rozmíchání složit do dvaceti tahů.

Literatura

[1] JAHODA, Pavel. Studijní materiály ke kurzu Algebra. *Webové stránky RNDr. Pavla Jahody, Ph.D.* [online]. [cit. 2019-04-26]. Dostupné z: http://k470.vsb.cz/jahoda/vyuka/algebra/

[2] GALLIAN, Joseph A. *Contemporary Abstract Algebra;* 4th ed.; Boston: Houghton Mofflin Company, c1998. ISBN 9780395861790.

[3] SCHERPHUIS, Jaap. *Jaap's Puzzle Page* [online]. 1999-2015 [cit. 2019-04-26]. Dostupné z: https://www.jaapsch.net/puzzles/

[4] TBROEDERS, Harry. The history of the 15 puzzle. *Homepage of Harry Broeders* [online]. 2014 [cit. 2019-04-28]. Dostupné z: https://hc11.home.xs4all.nl/15puzzle/15puzzen.htm

[5] BOGOMOLNY, Alexander. Sam Loyd's Fifteen. *Interactive Mathematics Miscellany and Puzzles* [online]. c1996-2018 [cit. 2019-04-28]. Dostupné z: https://www.cut-the-knot.org/pythagoras/fifteen.shtml

[6] CONRAD, Keith. The 15-puzzle (and Rubik's cube). *Keith Conrad* [online]. [cit. 2019-04-28]. Dostupné z: https://kconrad.math.uconn.edu/blurbs/grouptheory/15puzzle.pdf

[7] XYZZY. YJ Floppy Ghost Cube. *SpeedSolving.com* [online]. c2010-2018 [cit. 2019-04-26]. Dostupné z: https://www.speedsolving.com/forum/threads/yj-floppy-ghost-cube.66929/

[8] WALLOP, Harry. Rubik's cube invention: 40 years old and never meant to be a toy. *The Telegraph* [online]. Telegraph Media Group Limited, c2019 [cit. 2019-04-28]. Dostupné z: https://www.telegraph.co.uk/technology/google/10840482/Rubiks-cube-invention-40-years-old-and-never-meant-to-be-a-toy.html

[9] VAUGHEN, Christopher. Counting the Permutations of the Rubik's Cube. *Mathematics and the Rubik's Cube* [online]. [cit. 2019-04-28]. Dostupné z: https://faculty.mc3.edu/cvaughen/rubikscube/cube_counting.ppt

[10] ROKICKI, Tomas, Morley DAVIDSON, Herbert KOCIEMBA a John DETHRIDGE. *God's Number is 20* [online]. [cit. 2019-04-28]. Dostupné z: http://www.cube20.org/

[11] MULHOLLAND, Jamie. Permutation Puzzles: A Mathematical Perspective. *Jamie Mulholland* [online]. c2011 [cit. 2019-04-28]. Dostupné z: http://www.sfu.ca/ jtmulhol/-math302/notes/302notes.pdf

[12] Generating set of a group. *Groupprops, The Group Properties Wiki* [online]. 2017 [cit. 2019-04-26]. Dostupné z: https://groupprops.subwiki.org/wiki/Generating_set_of_a_group

[13] BEELER, Robert. The Fifteen Puzzle A Motivating Example for the Alternating Group: (Supplemental Material for Intro to Modern Algebra). *Robert A. Beeler, Ph.D.* [online]. [cit. 2019-04-28]. Dostupné z: http://faculty.etsu.edu/beelerr/fifteen-supp.pdf

Zdroje obrázků

- Obrázek 3: Maďarské prstence [online].
  Dostupné z: https://ruwix.com/pics/hungarian-rings-solution-01.png
- Obrázek 5: Patnáctka [online].Dostupné z: https://cs.wikipedia.org/wiki/Patn%C3%A1ctka#/media/File:15-puzzle.svg
- Obrázek 6: Rozložená patnáctka [online]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/3/39/15-puzzle-loyd.svg
- Obrázek 7: Hlavolam Floppy Ghost Cube [online].Dostupné z: https://cubezz.com/images/201709/goods_img/5448_G_1505455754529.jpg
- Obrázek 10: Rubikova kostka [online].
  Dostupné z: https://upload.wikimedia.org/wikipedia/commons/thumb/4/43/Rubik%27s_cube_almost_solved.svg/983px-Rubik%27s_cube_almost_solved.svg.png
- Obrázek 11: Rozložená Rubikova kostka [online].
  Dostupné z: https://upload.wikimedia.org/wikipedia/commons/b/bb/Rubiks_cube_by_keqs.jpg